12
Meldplicht datalekken

Aan de orde is de voortzetting van de behandeling van:
- **het wetsvoorstel Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) (33662)**.

De beraadslaging wordt hervat.

☐

Staatssecretaris **Dijkhoff**:
Mevrouw de voorzitter. Ik dank u en de andere leden dat u dit wetsvoorstel zo voortvarend hebt willen behandelen, en dat op een voor de senaat zo belangrijke en interessante dag.

De bescherming van de persoonsgegevens gaat de overheid aan het hart. Die gaat ook het kabinet aan het hart. Ik heb gemerkt dat die ook de Eerste Kamer aan het hart gaat. De Kamer ziet het belang in van een betere bescherming van de gegevens van personen, ook waar het gaat om de databescherming online. Het wetsvoorstel zoals het nu voorligt kent twee hoofdonderwerpen. Enerzijds is er die algemene meldplicht voor datalekken. Daarnaast is er sprake van een uitbreiding van de bevoegdheid van het CBP — dat gaat straks, als het wetsvoorstel is aanvaard, Autoriteit Persoonsgegevens heten — om bij overtreding een bestuurlijke boete op te leggen.

Over beide elementen is veel gezegd en geschreven. Dat is terecht, omdat het steeds zoeken is naar een balans tussen enerzijds de bepaaldheid van de wetgeving en anderzijds de reikwijdte van de bescherming van de persoonsgegevens van burgers. De nieuwe verplichtingen beogen de Autoriteit Persoonsgegevens, het huidige CBP, in staat te stellen om op te treden waar dat nodig is en, indien informatie op straat komt te liggen of mogelijk in verkeerde handen komt, zo snel mogelijk maatregelen te treffen om het lekken te beperken en de impact daarvan de verkleinen en te beperken.

De Kamer heeft hierover de nodige vragen gesteld. Ook schriftelijk is er al een uitgebreide wisseling van vragen en antwoorden geweest. Ik stel het op prijs om nu hier de vragen te beantwoorden, allereerst de vraag van mevrouw Ter Horst, die niet de validiteit van deze meldplicht in twijfel trok, maar zich wel afvroeg hoe het met al die andere meldplichten staat. Ik ga niet de rekensom herhalen die hierbij mogelijk is. Een aantal meldplichten bestaat en een aantal is in wording. Het aantal dat in wording is, vervangt bestaande. Het is zelfs zo dat deze meldplicht die in wording is, op termijn alweer zal worden vervangen door een andere die in wording is, namelijk op Europees niveau. Het is niet alleen maar cumulatief, maar ik kan het ook niet zo wegredeneren dat er maar drie overblijven; wij hebben straks gewoon een flink aantal meldplichten over. Dat heeft vooral te maken met een poging om toch enige differentiatie aan te brengen. Het gaat om de erkenning dat het wel uitmaakt of het de overheid zelf is, een justitiële dienst of de politie, of een net beginnende webwinkel. Wij leggen iedereen een algemene meldplicht op, die hier nu voorligt. Daarnaast zeggen wij dat voor specifieke sectoren, zoals telecom of overheid, zwaardere eisen gelden. Voor die sectoren geldt dus ook een verzwaarde meldplicht en een ander regime.

Je hebt dus verschillende plichten; het is niet een stelsel met een algemene plicht en daarvan afgeleide plichten. De meldplichten zijn in de tijd ontstaan. Het is niet geheel onlogisch dat het bij de telecom begonnen is en dat de meldplicht daar dus ook al wat langer bestaat. Nederland loopt op dit terrein niet achter, maar je ziet dat na verloop van tijd ook op Europees niveau de behoefte ontstaat om het breder, gemeenschappelijk en geharmoniseerd te regelen. Daardoor wordt daarin weer een stap gezet. Wij proberen het wel te stroomlijnen, maar wij gaan niet ons eigen niveau van bescherming lager maken omwille van de harmonisatie.

Mevrouw Gerkens heeft een vraag gesteld over de exacte bewaartermijn. Dat is lastig. De termijn is gesanctioneerd. Het gaat natuurlijk niet om het bewaren van al die gegevens of de privacy rond al die data. Het gaat echt om het lek. Wij vinden het dan wat te mager om de gedachte te laten postvatten: ik heb het bij de autoriteit gemeld, die bewaart het wel. Je hebt een eigen verantwoordelijkheid om te kunnen terugzien in de ontwikkeling van het bedrijf wat de voorgeschiedenis was. Was het de eerste keer? Is het een herhaalprobleem? Zit het in het falen van het beleid of is er niet genoeg aandacht voor? Heel bepaald vinden wij het dan ook lastig om het heel exact te doen, vooral omdat vanwege de technologie de bezwaarlijkheid van het bewaren van dit soort gegevens is afgenomen. Wij hebben het immers waarschijnlijk niet over rijen ordners die je tien jaar lang moet bewaren. Er zit een gradatie in het belang en de ernst van de zaak. Als we dit aan de verantwoordelijkheid laten van de ondernemer zelf, kan er ook intern lang genoeg worden teruggeblikt en kunnen er lessen worden geleerd uit wat er is gedaan met een vorig probleem.

De bewaarplicht op termijn zou ook nog het effect kunnen hebben dat de gegevens automatisch verwijderd worden na die termijn. Dat kan natuurlijk jammer zijn, in die gevallen waar het informatie betreft die nuttig kan zijn voor het voorkomen en verhelpen van toekomstige problemen.

Mevrouw **Gerkens** (SP):
Maar ik wil juist voorkomen dat mensen gegevens veel te snel weggooien. Misschien kan de staatssecretaris ons aangeven dat dergelijke gegevens minimaal een aantal jaar bewaard moeten worden. Op den duur zijn ze toch verouderd, want de systemen verouderen, maar ik kan mij voorstellen dat een minimale bewaartermijn van vijf jaar al behoorlijk redelijk is.

Staatssecretaris **Dijkhoff**:
Ik zoek dan een beetje aansluiting bij de Telecommunicatiewet, niet omdat daar wel een termijn in staat, maar omdat ook daar geen termijn in staat en de systematiek hetzelfde is. In de telecomsector gaan de ontwikkelingen erg snel, waardoor men zelf doorgaans een termijn van twee tot drie jaar hanteert. Dat heeft ook te maken met wat mevrouw

Gerkens al aangaf: de omloopsnelheid van systemen. Het lijkt me daarom verstandig dat een bedrijf zelf dat beleid voert en zelf bekijkt welke informatie erg systeemgebonden is en welke meer gebonden is aan de bedrijfscultuur. We denken echter wel in jaren en niet in maanden, al was het maar omdat, als er een sanctie aan gekoppeld is of als het proces van het informeren van burgers van wie de data potentieel in verkeerde handen zijn gevallen nog loopt, er tijd overheen gaat en je een jaarlijkse verantwoordingscyclus hebt. Je moet kunnen terugblikken om verantwoording af te kunnen leggen. Een exacte bewaartermijn, generiek, voorzie ik dus niet. Ik acht het heel wel mogelijk dat het CBP bij het vaststellen van de richtsnoeren en meer specifiek bij het type probleem een indicatie kan geven van de bewaartermijn. De Kamer kan daar dan over geïnformeerd worden.

Een andere vraag betrof de richtsnoeren. Deze worden samen met het kabinet vastgesteld. Er wordt vooraf over overlegd. Ze worden ook gepubliceerd. Wij zullen ervoor zorgen dat ze bij de Kamer terechtkomen, zodat de leden de richtsnoeren kunnen zien en er een mening over kunnen vormen. Als daar behoefte aan is, kunnen de leden er daarna over in overleg treden.

Mevrouw Gerkens vroeg ook om iedereen te informeren als de wet er is. Wij erkennen dat naast de gebruikelijke publiciteit rondom een nieuwe wet die van kracht is geworden, deze wet expliciete aandacht behoeft, al was het maar omdat het vaak om een datum gaat waarop ook veel andere wetten van kracht worden. Wij voorzien dat wij in overleg zullen treden met het CBP maar ook met de Kamer van Koophandel om te bekijken op welke manier we dit het beste kunnen doen. We moeten het niet laten bij alleen de publicatie van de wet zelf. Ik wil niet zover gaan dat ik nu toezeg dat het instrument van een brief op papier gericht aan het adres van inschrijving de meest geëigende weg is. Maar ik wil wel toezeggen dat wij voor ogen hebben om hier een brede bekendheid aan te geven, en dat niet slechts middels een eenmalige actie, zodat vooral ook in de sectoren waar het relevant is er brede aandacht is voor dit punt, hetzij rechtstreeks vanuit het ministerie, hetzij vanuit het CBP. Dat moet zich dan natuurlijk meteen presenteren als een instantie die deze bevoegdheid heeft. Ik permitteer mij even de vrijheid om voor het CBP te bedenken dat het zou kunnen zeggen dat het niet zal aarzelen om deze bevoegdheid te gebruiken.

Mevrouw **Gerkens** (SP):
Ik had de staatssecretaris nog de suggestie gegeven om daarbij te verwijzen naar het programma voor het mkb dat bij het ECP loopt. Is de staatssecretaris voornemens om dat te doen?

Staatssecretaris **Dijkhoff**:
Ja, zeker als wij zelf de communicatie ter hand nemen. Als wij de lead in de communicatie hebben, zullen wij ook onder de aandacht van het CBP brengen dat het niet alleen moet zeggen "er is een plicht; u moet het melden en als u dat niet doet, dan zwaait er wat", maar ook moet zeggen "hebt u hulp nodig, dan kan dat bij het CBP zelf, maar we hebben ook allerlei programma's lopen voor de implementatie".

Mevrouw Ter Horst had een vraag over een jaarlijkse rapportage van de aantallen gemelde datalekken. Zeker. Het CBP gaat ook de effecten monitoren, juist omdat we bij de behandeling hebben gemerkt dat er twee risico's zijn. Het eerste is het risico dat men denkt: het zal wel loslopen, dus we melden het niet. Het tweede is het risico dat men denkt: ik heb een brief gehad en het is mij ook anderszins duidelijk dat er iets zwaait, dus ik ga aan overcompliance doen. "Overcompliance" is een mooie managementterm om te beschrijven dat mensen zich te veel aan de regels houden. We willen die risico's kunnen voorzien en ze waar nodig bijsturen. Het jaarverslag zal die monitoring bevatten. Dat wordt ook gepubliceerd en aan het parlement aangeboden. Dan kan het dus verder onderwerp van gesprek zijn.

Ik kom op de vraag van mevrouw Gerkens over de structurele voorziening, een brief inzake de Hold-casus. Dit betreft een andere meldplicht dan waar mevrouw Ter Horst naar verwees in haar vraag, in de cybersecurityhoek, bij het NCSC. Die voorziening is opgenomen in het wetsvoorstel inzake de cybersecurity. Ik verwacht dat dit binnenkort in de ministerraad zal worden behandeld en dan naar de Raad van State zal worden verzonden voor advies.

De meeste vragen zijn gesteld over het lastigste onderwerp. Ik heb dat tot het einde bewaard, om er eerst even in te kunnen komen. Dat onderwerp betreft de spanning die er is tussen de bepaaldheid van de norm en de reikwijdte van de meldplicht. Maken we de wet heel specifiek, dan weet iedereen precies waar hij aan toe is, maar dan lopen we ook het risico dat binnen de kortste keren de ontwikkelingen in de praktijk en in de techniek ervoor zorgen dat we hier weer staan met een nieuw wetsvoorstel, omdat het oude net niet voorzag in die nieuwe ontwikkelingen. Het doel van de uitbreiding van de bevoegdheid van het CBP was dat het CBP de bevoegdheid kreeg om overtredingen van de gegevensbeschermingsbepalingen te kunnen bestraffen met boetes. Zo hoeft het niet alleen in het toezicht een waarschuwend vingertje te heffen, maar kan het ook een flinke boete opleggen, als dat echt nodig is en als er echt aanleiding toe is. Zo wordt de verantwoordelijke ter verantwoording geroepen en ervaart deze de consequenties. Een ander doel bij het inrichten van de systemen is altijd geweest om de verantwoordelijke niet een onmogelijke inspanning op te leggen. Hij moet niet uit hoeven puzzelen of hij wel of niet aan de wet voldoet. Die twee doelen leiden tot een spanning waarin je een balans moet vinden.

Een ander doel is om zo veel mogelijk mensen te beschermen en om de samenleving zo veel mogelijk ervan te doordringen dat het niet zo is dat het helemaal niet erg is als data ergens weglekken of dreigen weg te lekken. Uit de evaluatie van de Wet bescherming persoonsgegevens is naar voren gekomen dat dit punt steeds terugkomt en dat het vaak gaat om algemeen geformuleerde normen. Dat is een wat neutrale term, een ander noemt het "open" en weer een ander zelfs "vaag". Dat is het systeem, vooral ook omdat het vaak problemen zijn waar we nu voor het eerst tegenaan lopen en die zich nog moeten zetten in de samenleving. Dat maakt het lastig. Bedrijven kunnen niet meteen zien of hun gedrag wel of niet strafbaar dan wel beboetbaar is.

Een andere zaak waar wij als wetgever mee te kampen hebben, is de sterke afhankelijkheid van de context om te kunnen bepalen of iets daadwerkelijk een probleem is. De precieze omstandigheden van het geval zijn daar nogal

leidend in. Zeker, bij de toepassing van de richtlijnen moet rekening worden gehouden met het rechtszekerheidsbeginsel. We zien bij de ontwikkeling van het wetsvoorstel dat de checks-and-balances verschoven zijn. Het is niet letterlijk dezelfde tekst als die ooit als eerste werd ingediend. Dat heeft natuurlijk ook te maken met het feit dat de Afdeling advisering van de Raad van State erop gewezen heeft dat hier nog wel iets aan mocht gebeuren. Ook is erop gewezen dat als tussenstap een bindende aanwijzing gegeven moet worden. Er is inmiddels voor gekozen om de onbepaaldheid, het moeten inwerken en het moeten leren omgaan met deze materie niet terug te draaien, maar te compenseren door de stap van de bindende aanwijzing voordat er wordt overgegaan tot boetes. Ook is er gekozen voor de verplichting om de richtsnoeren niet alleen maar door het CBP zelf te laten ontwikkelen, maar het CBP ook op te dragen om hiervoor voorafgaand aan de vaststelling overleg te voeren met het kabinet, en wel met de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie, zodat het proces meer begeleid wordt. Er is dus voor gekozen om de onbepaaldheid op die manier te ondervangen.

Een interpretatieve verklaring daarvan, waar de heer Franken naar vroeg, vind ik op dit moment niet op zijn plaats, omdat wij juist hebben besloten om het samenstellen van de richtsnoeren in samenspel met het CBP te gaan doen en daarin de expertise uit het veld mee te nemen. Een andere reden waarom het gevraagde voor mij lastig is, is de volgende. Samenspel is mogelijk. Dat gebeurt ook op advies van de Raad van State. Maar we hebben ook de onafhankelijkheid van het CBP in acht te nemen. De Europese privacyrichtlijn schrijft dat nadrukkelijk voor. De ruimte om de wettelijke normen nader uit te werken tot op detailniveau is dus beperkt.

De heer **Franken** (CDA):
Ik vraag de staatssecretaris dan om eens duidelijk aan te geven wat de woorden "een aanzienlijke kans" betekenen. Ik heb een aantal voorbeelden gegeven van dergelijke redelijk vage formuleringen die in het recht voorkomen, op diverse rechtsgebieden. Maar zeg het nou eens in gewoon Nederlands. De burgers kennen die juridische abracadabra niet. Zegt u nou eens in gewoon Nederlands wat u "een aanzienlijke kans" vindt, staatssecretaris. Een kans van 60% dat het niet zal gebeuren? Of 100%? Probeer het nou eens gewoon te omschrijven, in gewone taal.

Staatssecretaris **Dijkhoff**:
Daarvoor is technologie te lastig. De kans dat er iets gestolen is bij een inbraak is aanzienlijk. Dat kan ik schatten. Ik ga dan gewoon naar de plek waar de deur open heeft gestaan en kijk of er iets weg is. Ik weet misschien niet precies wat er stond, maar ik weet het wel ongeveer. Ik weet dan dus of er iets weg is. Bij data is het anders. Dan kun je beter de vergelijking maken met iemand die een fysiek pand binnen is gegaan en er foto's heeft gemaakt. Dat kan ik niet zien. Een datalek betekent niet dat de weggelekte data verdwenen zijn. Daarvan is een kopie gemaakt. Technologisch hangt de kans af van de mogelijkheid om de in het systeem ontdekte kwetsbaarheid uit te nutten. Daarbij kan voor een hacker bijvoorbeeld de laagdrempeligheid om binnen te komen een rol spelen. De vraag is dan of nog niemand op deze kwetsbaarheid gestuit is of dat een ethische hacker die al in het kader van de "responsible disclosure" heeft aangemeld. Het kan ook gaan om een probleem waarover in de literatuur al tien jaar wordt geschreven en waarvoor heel veel updates, patches en reparatiewerk zijn geweest of ter verhelping waarvan juist niets is uitgevoerd. Er kunnen inmiddels al tooltjes zijn die niet alleen hackers maar ook wij in deze zaal voor een paar dollar kunnen kopen, om daarmee te scannen of een netwerk een dergelijke kwetsbaarheid vertoont. Naarmate de kwetsbaarheid groter is, stijgt de kans dat iets ontvreemd is. De inhoud van de data die aan kopiëren of hacken ten prooi zijn gevallen, draagt bij aan de mate waarin het gemeld moet worden. Als het gaat om een systeem met enkel de naam en het e-mailadres van een sportvereniging en het een heel gangbare sport is, is de kwetsbaarheid van de gegevens die in het geding zijn een stuk kleiner dan indien het gaat om misschien wel dezelfde combinatie van naam en e-mailadres, maar dan van een vereniging die maatschappelijk omstreden is, om maar iets te noemen, en waarvan het niet per se gangbaar is om lid te zijn. Het kan ook gaan om een webwinkel die producten verkoopt waarvan de gebruiker of de consument niet wil dat iedereen dat weet. Als je weet dat je dergelijke producten verkoopt, is je verantwoordelijkheid groter. De technische kans op een lek moet dan worden vermenigvuldigd met de kwetsbaarheid van de informatie om te kunnen analyseren of er sprake is van een verplicht te melden lekkage of risico op lekkage. Ook daar hebben wij het over. Als een vat olie lekt, kun je meten of er iets uit is, maar in dit geval kan er iets uit zijn zonder dat je het weet. Ook als je niet kunt vaststellen of er iemand is langsgekomen die gebruik heeft gemaakt van het lek om data te kopiëren, kan de kwetsbaarheid van de data er wel toe leiden dat het verplicht is om er melding van te maken. Dat heeft de Tweede Kamer zo geamendeerd.

De heer **Franken** (CDA):
Vindt de staatssecretaris de risicofactor bepalend? Ik zeg niet dat ik het daarmee niet eens zou zijn, maar dan geeft de staatssecretaris een bepaalde handreiking.

Staatssecretaris **Dijkhoff**:
Ja, risicofactor maal ernst. Risico is natuurlijk altijd de kans dat iets gebeurt maal de ernst van het gebeurde. Dat zit al in het woord "risico" ingebakken. In dit wetsvoorstel is inderdaad gekozen voor de risicobenadering.

In veel gevallen zal meteen duidelijk zijn dat melding verplicht is. In een aantal gevallen, waarvan de Kamer enkele voorbeelden heeft genoemd, is dat niet het geval. Waarop sturen wij nu? Wij sturen natuurlijk op melding van precies al die gevallen die binnen de bandbreedte vallen. Als we risico moeten nemen, met name in het begin, is het "better safe than sorry" niet alleen een risico in de samenleving, maar iets wat we vooral in het begin liever hebben dan dat er maatschappelijke ophef is doordat we moeten constateren dat er vanwege de reikwijdte en door een belangrijk en cruciaal lek gegevens op straat zijn komen te liggen zonder follow-up of melding aan de mensen die het betreft. Met deze instrumenten en dit kader van wetgeving heb ik er vertrouwen in dat het College bescherming persoonsgegevens de nieuwe door de wet geboden mogelijkheden goed kan benutten en mede een werkbare praktijk kan vormen, waarin bedrijven weten waar zij aan toe zijn en waarin vooral onze data goed beschermd worden.

Mevrouw Gerkens gaf mooi aan dat het hierbij natuurlijk niet alleen om bewuste fouten en wetsovertredingen gaat die als een crimineel nagejaagd moeten worden. Daarom zit het ook in het bestuurlijke regime. Criminelen maken misbruik van lekken die ontstaan. Het voorkomen van die lekken is natuurlijk veel beter dan het moeten melden ervan. Bewustwording in de samenleving is dus van cruciaal belang. Het is niet alleen zaak dat mensen een lek melden waarvan ze zelf weet hebben, maar ook dat zij mondig worden zodra zij zich afvragen waarom mensen iets willen weten overeenkomstig het voorbeeld van mevrouw Gerkens. Een dergelijke mondigheid zou ook moeten ontstaan als we denken dat er iets mis kan zijn. Als telkens wanneer ik iets zeg mensen ook maar één wachtwoord aanpassen, neemt de veiligheid al toe. Dat is mijn mantra. Het netwerk aan informatievoorzieningen dat we in Nederland hebben, valt of staat met de veiligheid in de gehele keten en niet alleen met de dingen die we kunnen vatten onder wettelijke bepalingen.

Hiermee kom ik aan de afronding van de beantwoording van de vragen. Indien de Eerste Kamer zich in het voorliggende wetsvoorstel kan vinden, zullen wij de uitwerking ervan met spoed ter hand nemen, richtsnoeren ontwikkelen en de wet in werking laten treden om de data van ons allen beter te beschermen.

☐

De heer **Franken** (CDA):
Voorzitter. Ik zal staccato een paar opmerkingen maken. De eerste is dat ik mijn positieve opmerkingen in de eerste termijn enigszins omfloerst heb gebracht, omdat de bestuurlijke aanpak van die heel hoge boete door niet-rechters waar wij meestal nogal tegenaan hikken, in een wat abstract kader geplaatst wordt. Voor alle duidelijkheid merk ik nog eens op dat wij blij zijn dat deze wet tot stand komt, waar het aan dit college is toegekend om dergelijke bevoegdheden uit te dragen en waar te maken. Ten tweede had ik toegezegd dat ik in tweede termijn nog met een enkele praktische vraag zou komen. Mevrouw Gerkens heeft die vraag al gesteld. Deze betreft het overzicht dat een verantwoordelijke moet bijhouden van de gemelde inbreuken. De bewaartermijn is niet voorgeschreven. In de memorie van antwoord is duidelijk gemotiveerd waarom dat niet zou moeten. De staatssecretaris is daarop nog eens ingegaan. Mevrouw Gerkens heeft gezegd dat je toch aan minstens vijf jaar moet denken. Mij lijkt dat erg veel. Ik zou als criterium aan willen houden dat de gegevens zolang bewaard moeten worden dat er voor het College bescherming persoonsgegevens een redelijke mate of misschien zelfs aanzienlijke mate, om maar een bekende kreet uit artikel 34 over te nemen, is om goed onderzoek te verrichten. Als zij niet gedurende een jaar worden opgeslagen, lijkt mij de kans voor het CBP gering. Het overzicht zal dus minimaal een jaar moeten worden bijgehouden en bewaard. Hierover hoor ik graag een toezegging van de staatssecretaris.

Mijn derde punt betreft de hoofdmoot van mijn inbreng, dus de interpretatieve verklaring van artikel 34a. De staatssecretaris heeft geprobeerd om tussen Scylla en Charybdis door te varen. Dat kan ik mij wel voorstellen, maar het punt is dat de gewone burger met deze vraag zit. Het lijkt mij dat het al iets duidelijker is als die erop is gewezen dat er een bepaald risico aan de orde moet zijn, te meer daar er zelfs een handel in lekken plaatsvindt, zoals de staatssecretaris misschien bekend is. Die heet "zero-day exploits". Zij schijnt nogal lucratief te zijn. Er wordt dan een bepaald risico van een ander verkocht. Ik zou dat bijna een criminele daad noemen, maar zo kunnen wij dit nog niet kwalificeren.

Mijn vierde punt betreft het Engelse woord "awareness", waarvan ik denk dat het zo langzamerhand een Nederlands woord moet worden. Wij moeten ons zo bewust zijn van de schade die men kan lijden door het verkeerd gebruiken van informatietechnologie of door het feit dat anderen die verkeerd gaan gebruiken, dat ik dat woord ingelijst en wel boven het bed van eenieder wil hangen. Dan ziet iedereen dat bij het slapen gaan en bij het opstaan wederom.

Het melden van datalekken is een onderdeel van de borging van het vertrouwen dat mensen nodig hebben om te communiceren. Vertrouwen is de basis van onze samenleving. Ik ben verheugd dat wij deze middag een bijdrage hebben kunnen leveren aan de borging daarvan.

De **voorzitter**:
Dank u, mijnheer Franken. Voordat ik mevrouw Ter Horst het woord geef voor haar bijdrage in tweede termijn, merk ik op dat ik begrepen heb dat dit uw laatste woorden in deze samenstelling van de Eerste Kamer waren. Bij een vorig debat hebben wij het ook al gezegd, maar ik herhaal het bij dezen: wij zullen u node missen.

(Geroffel op de bankjes)

☐

Mevrouw **Ter Horst** (PvdA):
Ik ben benieuwd wat de voorzitter gaat zeggen als ik ben uitgesproken!

De **voorzitter**:
Dat wij u ook zullen missen!

Mevrouw **Ter Horst** (PvdA):
Maar niet node! Ik hoor het al!

De **voorzitter**:
Dat is met name vanwege de expertise van de heer Franken op dit terrein.

Mevrouw **Ter Horst** (PvdA):
Absoluut. U hoeft het niet uit te leggen, hoor.

Voorzitter. Ik had eigenlijk niet zo vreselijk veel behoefte aan een tweede termijn. Ik dank de staatssecretaris voor zijn beantwoording. Ik begrijp uit zijn woorden dat niet alle organisaties aan alle meldplichten moeten voldoen. Je mag ze dus niet allemaal bij elkaar optellen. Ik denk dat wij de staatssecretaris wel mogen zien als iemand die er alles aan zal doen om ervoor te zorgen dat de druk om te melden die op organisaties wordt gelegd, zo gering mogelijk is. Ik heb daar alle vertrouwen in.

Ik heb de staatssecretaris ook horen zeggen dat het College bescherming persoonsgegevens de effecten gaat monitoren en die in een jaarverslag zal vastleggen. Ik hoop dat ik het niet gemist heb, maar volgens mij is de staatssecretaris

niet ingegaan op mijn verzoek om nu al iets te zeggen over de richtsnoeren waarmee het College bescherming persoonsgegevens komt. Heeft hij daar al een beeld van? Mocht die vraag te ingewikkeld zijn, aangezien hij daarop in eerste termijn niet is ingegaan, dan zou ik graag horen of hij de bereidheid heeft om de richtsnoeren aan de Kamer ter beoordeling te zenden als ze daadwerkelijk tot stand zijn gekomen.

De **voorzitter**:
Dank u wel, mevrouw Ter Horst. Wij zullen u missen! Het woordje "node" sla ik inderdaad over. Wij zullen u — en dat meen ik oprecht — missen!

(Geroffel op de bankjes)

De **voorzitter**:
Ik heb begrepen dat u geen behoefte had aan een bijdrage in tweede termijn, mevrouw Gerkens? Wij zien u tenslotte ook nog terug in de Kamer in haar volgende samenstelling.

Dan geef ik nu het woord aan de staatssecretaris.

☐

Staatssecretaris **Dijkhoff**:
Voorzitter. Ik voel bij de sprekers steun voor en vertrouwen in het wetsvoorstel. Ik hoop dat dit uiteindelijk zal blijken, zodat wij snel aan de slag kunnen gaan.

De heer Franken heeft gevraagd of ik kan toezeggen dat de termijn minimaal een jaar is. Ik kan toezeggen dat ik deze wens zal overbrengen in het gesprek met het College bescherming persoonsgegevens, dat zijn richtsnoeren hieromtrent zelfstandig maar wel in overleg moet vaststellen. Ik deel deze wens ook; een jaar is wel het minste. Zoals ik al zei, wordt in de sector zelf vaak twee à drie jaar logisch gevonden. Wel wil ik dit in richtsnoeren ook brengen als een eigenstandige verplichting voor de organisatie, niet alleen gekoppeld aan de mogelijkheid tot het doen van onderzoek, om te voorkomen dat een organisatie denkt: ik heb het gemeld, dus neem aan dat ze het zelf bewaren. Het gaat namelijk om het bewaren van aan het CBP gemelde datalekken.

Wat de heer Franken heeft opgemerkt over de handel in lekken is allemaal waar. Awareness en bewustwording zijn belangrijk. Dat ben ik geheel met de heer Franken eens. Ik voeg daaraan toe dat het dan ook aan ons is om aan te vullen waarvan wij ons bewust moeten worden. In dit geval is dat zeker ook de eigen bijdrage die wij allemaal moeten leveren aan een veiligere communicatie onderling.

Mevrouw Ter Horst vroeg of ik een beeld had van de richtsnoeren. Ik heb haar eerdere vraag te impliciet behandeld, dus het lag aan mij. Ik heb namelijk wel gezegd dat ik de richtsnoeren naar de Kamer zal sturen zodra ze er zijn en gepubliceerd worden. Daarmee impliceerde ik inderdaad dat ik er op dit moment geen zicht op heb en dat ik nog geen informatie kan geven over de inhoud van de richtsnoeren in ontwikkeling. Het college heeft in het overleg met het kabinet aangegeven dat het hiervoor goed de tijd wil krijgen om dit de komende maanden uit te voeren, zodat de richtsnoeren duidelijk zijn zodra het wetsvoorstel van kracht wordt en zodat wij geen tijd hebben waarin er wel een wet is maar nog geen duidelijkheid voor burgers en bedrijven over de precieze bedoelingen daarvan.

De beraadslaging wordt gesloten.

De **voorzitter**:
Het wetsvoorstel wordt zonder stemming aangenomen.

Ik complimenteer de staatssecretaris met de prachtige winst, waarmee ik deze vergadering kan afsluiten.